panduan perlindungan digital untuk aktivis

kemitraan partnership
imparsial THE INDONESIAN HUMAN RIGHTS MONITOR
SAFEnet SOUTHEAST ASIA FREEDOM OF EXPRESSION NETWORK
ELSAM
kemudi
ICW INDONESIA CORRUPTION WATCH
</purplecode>

PANDUAN PERLINDUNGAN DIGITAL UNTUK AKTIVIS

Penulis:

1. Ellen Kusuma
2. Resa Temaputra
3. Wana Alamsyah
4. Blandina Lintang Setianti
5. Firman Imaduddin

Penasihat:

1. Dhyta Caturani
2. Swandaru

Sampul, tata letak, dan ilustrasi: Gendis Kendra Disa

Dokumen bersama Imparsial, SAFEnet, ELSAM, Kemudi, Indonesia Corruption Watch, dan Purple Code.

PENERBIT IMPARSIAL, The Indonesian Human Rights Monitor
Jl. Tebet Dalam IV J No.5B, Jakarta Selatan 12810
Phone : (+62-21) 829 0351
Fax : (+62-21) 285 41821
Email : office@imparsial.org
www.imparsial.org

Didukung oleh:
Kemitraan

Panduan Perlindungan Digital untuk Aktivis oleh Ellen Kusuma, Resa Temaputra, Wana Alamsyah, Blandina Lintang Setianti, Firman Imaduddin berlisensi di bawah **CC BY-NC-ND 4.0**.

Publikasi ini boleh direproduksi dengan bebas, dikutip dengan bebas, dan disebarkan dalam segala bentuk dan cara, elektronik atau mekanis, termasuk fotokopi, cetakan, rekaman, dan segala sistem penyimpanan informasi tanpa perlu meminta izin langsung dari penerbit, selama konten tidak diubah atau diatribusikan pada sumber yang lain.

DAFTAR ISI

01	DAFTAR ISI
03	PENGANTAR
06	KASUS-KASUS SERANGAN DIGITAL
07	Gawai/Telepon Genggam/Komputer
08	Situs *Web*, Data dan Akun Digital
09	Psikososial dan Legal
11	MENYUSUN STRATEGI KEAMANAN
12	Keamanan Personal
13	**Penilaian Risiko**
13	Identifikasi Aset dan Aplikasi
16	Kenali juga Konsep Data Pribadi/PII (*Personal Identifiable Information*)!
20	Identifikasi Ancaman
22	**Menyusun Strategi**
22	1. Gawai/Komputer
32	2. Situs *Web*, Data dan Akun Digital

34 3. Perilaku Aman
38 4. Menghadapi Ancaman yang Terjadi
48 5. Lapor

50 Keamanan Organisasi/Sistem
52 Lakukan Analisis Risiko Organisasi
52 Inventarisasi Aset Informasi
53 Identifikasi Aset dan Aplikasi
55 Klasifikasi Informasi Kunci yang Dimiliki Organisasi
56 Identifikasi Ancaman

58 Manajemen Manusia

60 Kebijakan Akses
60 1. Akses ke Tempat Kerja
62 2. Akses ke Dokumen Fisik
62 3. Perangkat
64 4. Akses ke Internet
66 5. Akses ke Akun Digital
69 6. Kebijakan Manajemen Data (RS)
74 7. Perjalanan ke Luar Daerah/Negeri
78 8. Praktik dan Kebijakan Komunikasi

82 GLOSARIUM

Pengantar

Kepada teman-teman pembela HAM,

Dalam kerja-kerja aktivisme dan advokasi kita, internet telah membuka begitu banyak peluang baru. Akses terhadap informasi atau kelompok yang dulu hanya dapat kita khayalkan, atau membutuhkan ongkos dan tenaga yang sangat besar, kini dapat diperoleh melalui ujung jempol di telepon pintar kita.

Namun bersama peluang baru, hadir pula ancaman baru. Dari sifat pekerjaannya, pembela HAM seringkali sudah rentan terhadap serangan. Ketika aktivitas pembela HAM semakin berpindah ke dunia digital, ancaman yang kita hadapi ikut bermigrasi ke dunia digital.

Bentuk ancaman-ancaman ini juga semakin bervariasi. Mulai dari ancaman peretasan situs web dan pencurian data yang mengganggu aktivitas advokasi, hingga pembocoran dan manipulasi data pribadi yang berujung kriminalisasi, intimidasi, atau bahkan kekerasan fisik.

Menghadapi tantangan baru ini bukan hal mudah. Banyak kelompok dan pembela HAM menganggap bahwa ancaman semacam ini adakah "risiko wajar" bagi aktivis, belum memiliki kesadaran dan pengetahuan terkait keamanan digital, atau sekadar tidak memiliki cukup waktu dan tenaga untuk didedikasikan dalam menghadapi ancaman digital.

Padahal, ada banyak langkah sederhana yang dapat dilakukan untuk meningkatkan keamanan bersama pembela HAM. Karena itulah kami dari Imparsial, SAFEnet, ELSAM, Kemudi, Indonesia Corruption Watch, dan Purple Code Collective berkolaborasi untuk membuat buku saku ini.

Kami berharap bahwa buku ini dapat meningkatkan kemampuan rekan-rekan pembela HAM dengan tetap menimbang beragamnya sumber daya dan pemahaman yang dimiliki oleh pembela HAM di seluruh penjuru Indonesia.

Keamanan digital adalah isu yang senantiasa berubah dengan cepat. Karena itu dokumen ini akan diperbarui secara rutin agar terjaga relevansinya dengan ancaman dan strategi keamanan digital terbaru.

Untuk memberi masukan terkait perkembangan panduan ini, harap hubungi tim penulis yang berasal dari organisasi-organisasi pemilik dokumen:

Firman Imaduddin (Imparsial)
firmanimad@imparsial.org

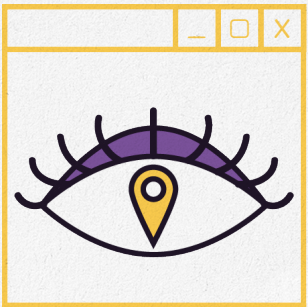
Ellen Kusuma (SAFEnet)
info@safenet.or.id

Resa Temaputra (Kemudi)
resaaa@protonmail.com

Wana Alamsyah (Indonesia Corruption Watch)
grldnryn@protonmail.com

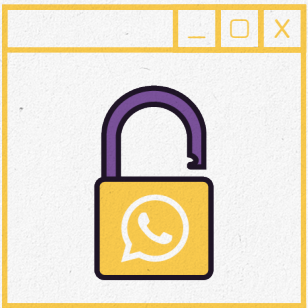
Blandina Lintang Setianti (ELSAM)
lintang@elsam.or.id

KASUS-KASUS SERANGAN DIGITAL

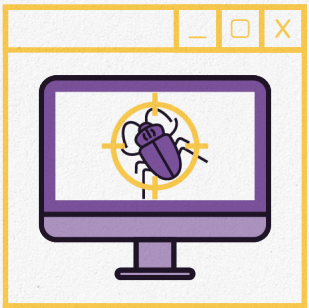


Pelacakan lokasi dan *surveillance*

Gawai/ telepon genggam/ komputer

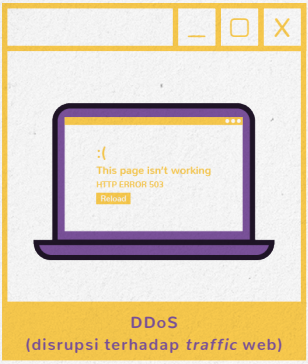


Peretasan kanal komunikasi (misal: WhatsApp)



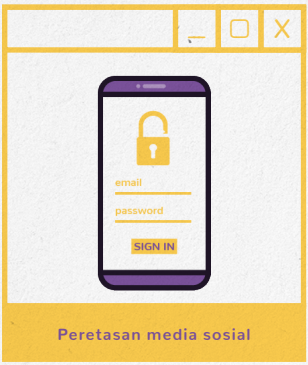
Virus, *malware*, dsc.

Situs web, data dan akun digital

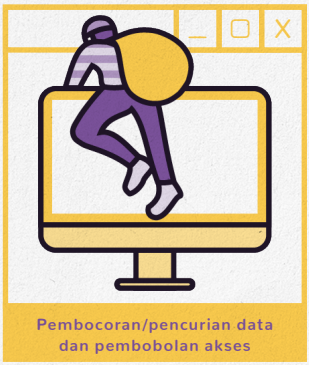


DDoS
(disrupsi terhadap *traffic* web)

Peretasan situs web



Peretasan media sosial



Pembocoran/pencurian data
dan pembobolan akses

Psikososial dan legal

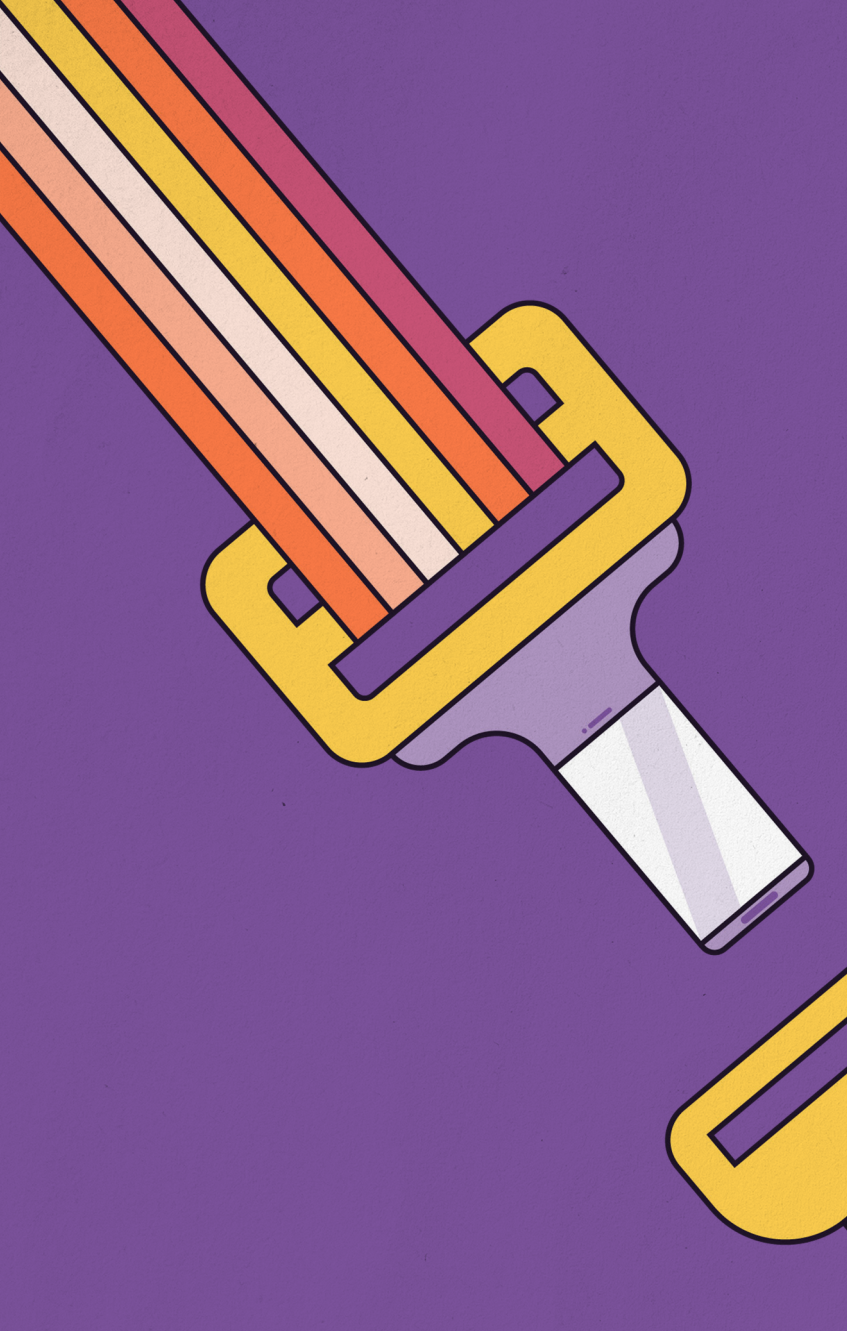
- KRIMINALISASI

- PEMBLOKIRAN

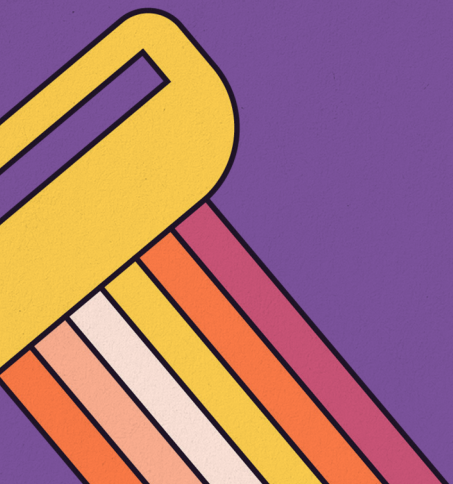
- PERISAKAN DAN INTIMIDASI DARING

- *DOXXING* (PEMBONGKARAN IDENTITAS)
- PENYALAHGUNAAN/ PENCURIAN IDENTITAS PRIBADI (KARTU KREDIT, NAMA/IDENTITAS)

- HOAKS DAN *SMEAR CAMPAIGN*



MENYUSUN STRATEGI KEAMANAN

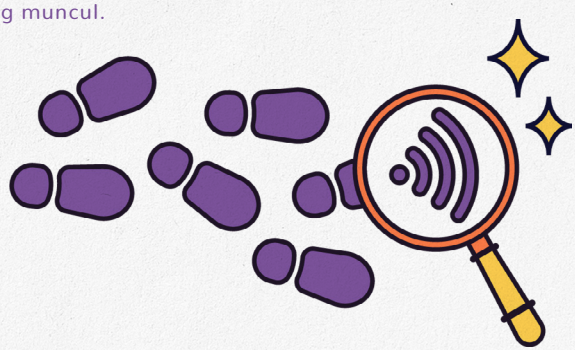


Keamanan Personal

Sebagai pembela HAM, Anda harus sadar bahwa aktivitas advokasi yang Anda lakukan punya potensi risiko tinggi. Bukan hanya risiko fisik, melainkan juga digital. Oleh sebab itu, penting bagi Anda untuk punya strategi keamanan digital untuk aktivitas personal saat melakukan advokasi.

Penilaian Risiko

RISIKO TIDAK DAPAT DIHILANGKAN, TAPI DAPAT DIMINIMALISIR. Penilaian risiko penting dilakukan supaya Anda dapat melakukan mitigasi terhadap setiap ancaman yang muncul.



IDENTIFIKASI ASET DAN APLIKASI

Bagaimana melakukan analisis risiko? Mulai dengan identifikasi aset dan peralatan yang Anda gunakan dalam aktivitas digital. Hal ini akan berdampak besar pada strategi keamanan yang perlu Anda susun. Coba buat ulang daftar ini:

1	**Gawai**	
	Handphone	
	Laptop	
	Tablet	
	Komputer personal (PC)	
2	**Media sosial**	
	Facebook	
	Instagram	
	Twitter	
	Dll., sebutkan	
3	**Layanan surel**	
	Gmail	
	Yahoo mail	
	Hotmail	
	Dll., sebutkan	
4	***E-banking***	
5	**SIM card**	
6	***File sharing* atau *cloud storage***	
	Google Drive	
	Dropbox	
	Dll., sebutkan	

7	**Aplikasi pesan**	
	LINE	
	Telegram	
	WhatsApp	
	DII., sebutkan	
8	**Aplikasi layanan transportasi**	
	Gojek	
	Grab	
	DII., sebutkan	
9	**Aplikasi manajemen kata sandi**	

KENALI JUGA KONSEP DATA PRIBADI/ PII (*PERSONAL IDENTIFIABLE INFORMATION*)!

Data pribadi adalah segala bentuk data yang dapat memberikan digunakan untuk mengidentifikasi seseorang. Data ini berhubungan erat dengan kemungkinan kebocoran data dan pencurian identitas. Ia juga membuka risiko besar serangan digital, intimidasi, atau bahkan serangan fisik pada individu terkait.

Data pribadi adalah "tubuh" Anda di dunia digital.

Data pribadi adalah "tubuh" Anda di dunia digital. Penting untuk kita mengenali baik-baik kehadiran tubuh digital kita di internet. Seberapa banyak tubuh digital kita atau data pribadi yang dapat diakses publik dengan mudah di internet? Apakah Anda aman dan nyaman dengan tingkat ketersediaan tersebut?

Tipe Data Pribadi	Contoh
Nama	Nama lengkap, nama kecil, nama ibu, alias
Nomor identitas pribadi	NIK, NPWP, SIM, plat kendaraan, nomor kendaraan, rekening bank, kartu kredit
Alamat	Alamat rumah, alamat kantor
Kontak pribadi	Email, nomor ponsel, nomor telepon rumah
Karakteristik	Foto, deskripsi penampilan
Data biometrik	Pindaian retina, tanda suara, sidik jari
Informasi atas properti pribadi	Akta tanah dan bangunan
Informasi aset teknologi	Alamat IP (*Internet Protocol*)
Lainnya	Tanggal dan tempat lahir, ras, agama, indicator geografis, dan informasi terkait pekerjaan, kesehatan, pendidikan, dan keuangan.

CATATAN:

Level aman dan nyaman seseorang dapat berubah seiring waktu dan konteks terkini kehidupan diri, sehingga perlu secara rutin melakukan cek dan ricek jejak digital masa lalu, seperti postingan status, foto, hubungan pertemanan di media sosial, dan lainnya. Semakin banyak informasi data pribadi diri yang bisa digali dari jejak digital di masa lalu, maka tingkat kerentanan semakin tinggi.

Coba jawab pertanyaan-pertanyaan ini!

1. Berapa akun digital yang Anda miliki?
2. Pernahkah Anda melakukan pencarian nama Anda sendiri di Google? Apa saja informasi pribadi Anda yang dengan mudah didapatkan di sana?
3. Apakah nomor ponsel dan alamat email kerja Anda terpisah dengan ponsel dan email pribadi?
4. Bagaimana pengaturan keamanan dan privasi dari akun digital dan media sosial Anda?
5. Apakah Anda punya akun digital yang masih aktif, namun tidak pernah digunakan?
6. Apakah alamat email atau data pribadi lain Anda pernah masuk daftar PII yang bocor?

PII yang bocor bisa dicek dengan memasukkan alamat email di https://monitor.firefox.com/ atau https://haveibeenpwned.com/.

Lebih lanjut, klasifikasikan data pribadi Anda ke dalam kategori-kategori ini. Pertimbangkan konteks-konteks khusus Anda: apa aktivitas digital Anda? Apa risiko dan kerentanan spesifik Anda? Klasifikasi data ini bisa menjadi sangat bervariasi jika menimbang konteks tersebut.

- Vital : Data yang sangat sensitif, yang dapat menimbulkan dampak luar biasa di tangan yang salah. Akses ini sebisa mungkin hanya dimiliki oleh pemilik data atau orang lain yang aman ketika sangat diperlukan. (Contoh: Pin rekening, kartu kredit, sandi akun digital).

- Pribadi : Tidak sesensitif data vital, namun tetap memiliki potensi kerusakan jika berada di tangan yang salah. (Contoh: Alamat, Tempat kerja, Kartu identitas, Tanda tangan, dll).

- Publik : Data non-sensitif dengan risiko minim. (Contoh: Nama panggilan).

IDENTIFIKASI ANCAMAN

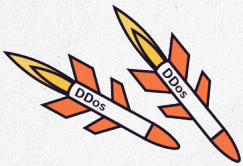
Setelah pemetaan aset digital yang dimiliki, saatnya bagi Anda untuk mengetahui apa saja risiko ancaman yang berpotensi Anda hadapi. Semakin banyak aset digital dan informasi pribadi Anda yang tersedia di internet, pertimbangkan untuk semakin memperdalam praktik kebijakan keamanan pribadi yang terkait. Berikut ini adalah contoh dari ancaman yang perlu Anda pertimbangkan:

1. Penyadapan atau pembobolan fisik

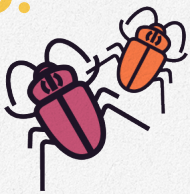
2. *Phishing*

3. Peretasan

4. Peretasan web atau disrupsi *traffic* web (DDoS)



5. Virus, *Malware*, *Spyware*



6. Pelacakan lokasi dan *surveillance*

7. Intersepsi komunikasi

8. *Doxxing* (pembeberan identitas pribadi kepada publik)

9. Perisakan dan intimidasi

10. Kriminalisasi atau *smear campaign*

Menyusun Strategi

Setelah mengidentifikasi risiko, Anda perlu menyusun strategi keamanan. Strategi ini perlu disusun berdasarkan aset apa saja yang Anda miliki dan gunakan.

Perubahan Perilaku dan Pola Pikir

Saat adanya serangan yang menimpa dirimu, sesungguhnya bukan hanya Anda yang terancam, tapi juga orang-orang yang berada di sekitarmu. Untuk melindungi mereka, perubahan perilaku dan pola pikir sangat diperlukan.

1. GAWAI/KOMPUTER

a. **Kata Sandi dan Keamanan Akses**

Buatlah kata sandi yang **kuat**. Buatlah kata sandi lebih dari **15 karakter dengan perpaduan simbol, huruf besar, huruf kecil dan angka**.

Untuk perangkat, **jangan gunakan kata sandi dengan menggunakan biometrik, seperti sidik jari dan retina**. Hindari kata sandi dengan angka karena polanya mudah terlihat.

Jika Anda sulit mengingat kata sandi, Anda dapat membuatnya dengan **model frasa**. Misalnya: **Bakso Pak Ujang di DEPAN sekolah, 3nak!**

REKOMENDASI Gunakan 1 kata sandi untuk 1 akun, jangan menggunakan kembali untuk akun lain. Keepass dapat membantu Anda untuk melakukan hal ini.

Dua cara lain mengingat kata sandi yang sulit adalah:
Pertama, simpan kata sandi di buku. Meski ada risiko buku tersebut hilang/basah/terbakar/dicuri.
Kedua, simpan di aplikasi manajemen kata sandi.

HINDARI Menggunakan manajemen kata sandi yang disinkronisasi secara online dengan akun digital lain (misal: manajemen kata sandi di dalam peramban Chrome yang disinkronisasi dengan akun Google atau Gmail yang dimiliki).

REKOMENDASI *Gunakan manajemen kata sandi yang tidak disinkronisasi secara daring*. Salah satunya adalah KeePassXC. Yang selain menyimpan kata kunci dapat juga menyimpan dokumen penting yang sudah di-*scan*.

KeePassXC untuk Windows, macOS, Linux, dapat diunduh di https://keepassxc.org/download/.

PERINGATAN:

JANGAN LUPA KATA SANDI UNTUK MEMBUKA APLIKASI. JIKA ANDA LUPA KATA SANDI MAKA APLIKASI YANG MEMUAT SEJUMLAH KATA SANDI TIDAK DAPAT DIAKSES.

Informasi lain yang dapat membantu Anda membuat kata sandi yang aman dapat dibaca di sumber berikut:

- Diceware
- Electronic Frontier Foundation (EFF) Dice-Generated Passphrases
- Panduan EFF tentang membuat *password* yang kuat
- Diceware Password Generator
- Panduan membuat *password* yang kuat oleh Security in a Box
- Komik oleh XKCD

Jika Anda ingin mengetahui seberapa kuat kata sandi, silakan cek di https://www.security.org/how-secure-is-my-password/.[1]

[1] Jangan menggunakan kata sandi asli yang Anda miliki. Gunakan pola kata sandi yang Anda gunakan. Tidak ada jaminan bahwa situs tersebut tidak menyimpan informasi, meskipun sudah ada pemberitahuannya.

b. **Enkripsi**

Upaya untuk memastikan keamanan saat pengiriman pesan ataupun data dengan sandi atau kode sehingga hanya bisa dibaca oleh pihak yang memiliki kode sandi atau kunci deskripsinya.

Enkripsi Pesan

Jangan gunakan SMS untuk informasi sensitif. SMS adalah layanan yang paling mudah dikuasai informasinya oleh pelaku.

SMS adalah layanan yang paling mudah dikuasai informasinya oleh pelaku.

REKOMENDASI Gunakan aplikasi pesan yang menggunakan *End-to-End Encryption* (E2EE), seperti Signal, Wire, atau Telegram, yang menjamin percakapan yang terjadi di dalam aplikasi tersebut hanya dapat dibaca antar pengirim dan penerima pesan saja.

CATATAN:
Aplikasi yang dapat di-*back-up* atau dicadangkan menggunakan aplikasi pihak ketiga, perlu dicek juga terkait dengan keamanan tempat *back-up* tersebut. Misal: Pesan WhatsApp yang dapat di-*back-up* secara lokal (di penyimpanan internal ponsel atau penyimpanan eksternal seperti *memory card*), maka ponsel dan *memory card* tersebut harus diperhatikan keamanannya.

Bila dicadangkan di *cloud storage* (seperti: Google Drive), perhatikan bahwa kebanyakan *cloud storage* tidak melakukan enkripsi pada data yang disimpan, sehingga perlu melakukan tindak keamanan lain agar data yang dicadangkan tersebut tidak dapat diakses orang lain, misal dengan melakukan enkripsi data terlebih dulu sebelum diunggah ke *cloud storage*, atau memastikan keamanan *cloud storage* tersebut dengan memastikan kata sandi yang kuat, mengaktifkan 2FA.

[BACA lebih lanjut tentang enkripsi dan manajemen data di Bab Kebijakan Manajemen Data (RS)]

c. **2FA**

Gunakan aplikasi layanan pesan yang memiliki fitur 2 *Factor Authentication* (2FA) atau Autentikasi 2 Faktor[2], yakni pengaman berlapis yang membuat akun Anda tidak mudah dibobol hanya lewat kata sandi. Istilah 2FA juga dikenal dengan istilah lain, seperti 2 *Steps Verification* (Verifikasi 2 Langkah).

Ada 3 faktor pengamanan terhadap keamanan digital:

1. Sesuatu yang Anda tahu, yaitu kata sandi, PIN, *passphrase.*
2. Sesuatu yang Anda miliki, yaitu alat verifikasi seperti OTP melalui SMS atau aplikasi autentikator dan kunci fisik.
3. Sesuatu yang merupakan diri Anda, yaitu biometrik (sidik jari dan pengenalan muka/retina).

2FA berarti menggunakan setidaknya 2 dari 3 faktor ini. Umumnya, untuk keamanan, faktor 1 dan 2 paling sering diprioritaskan.

Hindari menggunakan 2FA dengan metode OTP melalui SMS. Sebab, OTP merupakan informasi yang sensitif. Sedangkan SMS adalah layanan yang paling mudah dikuasai oleh pelaku. Gunakan 2FA pihak ketiga seperti Free OTP, Authy, dll.

[2] Lihat di https://www.securemessagingapps.com/.

Tautan ke sumber informasi terkait cara mengaktifkan 2FA:

- Tautan cara mengaktifkan 2FA di Google/Gmail
- Tautan cara mengaktifkan 2FA di Facebook
- Tautan cara mengaktifkan 2FA di Instagram
- Tautan cara mengaktifkan 2FA di Twitter
- Tautan cara mengaktifkan 2FA di WhatsApp

Sumber informasi lain terkait fitur 2FA di berbagai layanan dan platform:

- Two Factor Auth
- https://ictwatch.id/2fa

Beberapa layanan/*platform* menyediakan kode cadangan jika perangkat hilang dan dicuri. Pastikan Anda menyimpannya di tempat yang aman, kode cadangan tersebut dapat digunakan jika terjadi keadaan darurat.

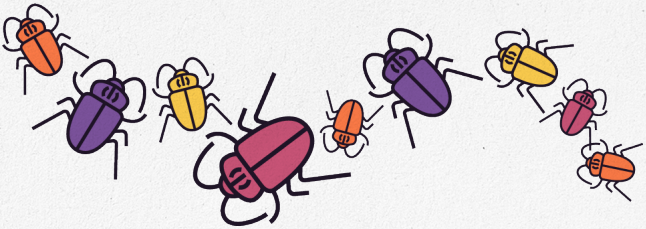
Informasi mengenai kode cadangan:

- Google dapat dilihat di sini.
- Facebook dapat dilihat di sini.
- Instagram dapat dilihat di sini.
- Twitter dapat dilihat di sini.

d. Pengamanan Virus dan Malware

Jangan pernah klik tautan yang tidak diketahui identitas pengirimnya. Ia bisa mengandung virus dan/ atau *malware*.

Pasang anti-virus untuk mengamankan seluruh perangkat Anda. **Selalu lakukan pembaharuan (*update*) terhadap aplikasi anti-virus** pilihanmu.



Identifikasi aplikasi yang telah ter-*install* atau terpasang di perangkat milikmu. **Jika ada aplikasi yang ter-*install* dan Anda merasa tidak pernah *install*, segera *uninstall* aplikasi tersebut**.

Jika Anda ingin melakukan pengecekan terhadap ***file* dan/atau tautan** yang Anda **dapatkan** dari orang yang **dikenal**, Anda bisa cek di https://www.virustotal.com/gui/ atau https://urlscan.io.

Latih sensitivitas untuk mengecek potensi email yang disisipi modus *phishing* dengan mengunjungi laman https://www.phishingbox.com/phishing-iq-test atau mengikuti kuis *phishing* yang disediakan Google di https://phishingquiz.withgoogle.com.

e. **Mengenali Aplikasi dalam Gawai**
Baca syarat dan ketentuan sebelum meng-*install* aplikasi.

Penting diperhatikan jika syarat dan ketentuan meminta **hak akses bagi pihak ketiga untuk mengakses sejumlah fitur di perangkat, seperti galeri foto, kontak, kamera, GPS, dll**. Jika aplikasi tersebut meminta akses fitur yang menurut Anda tidak relevan, pertimbangkan untuk tidak meng-*install*.

f. **Mengatur Privasi dan Keamanan**
Gunakan VPN setiap kali Anda menggunakan perangkat Anda. **Non-aktifkan GPS jika tidak diperlukan**.

Jangan pernah masuk ke dalam WiFi publik tanpa kata sandi.

Gunakan ekstensi untuk berselancar (HTTPs Everywhere, Ghostery-Privacy Ad Blocker).

REKOMENDASI Lakukan pengecekan dan penyesuaian pengaturan keamanan dan privasi di setiap akun digital yang dimiliki. Ada berbagai macam fitur keamanan dan privasi yang disediakan oleh masing-masing *platform* digital yang bisa disesuaikan dengan tingkat keamanan personal. Misal: Fitur matikan komentar, fitur membisukan pertemanan, dan lainnya.

g. Penggunaan Aplikasi Peramban

Gunakan peramban yang menjaga privasi seperti **ToR Browser, DuckDuckGo, Firefox, Brave. Matikan fitur lokasi** yang ada di dalam peramban milikmu.

Jika Anda ingin melakukan pencarian informasi, coba gunakan mesin pencari yang menjaga privasi seperti **DuckDuckGo** di https://duckduckgo.com/ atau dengan tidak melakukan *login* pada peramban yang digunakan serta senantiasa menghapus riwayat pencarian setelah digunakan.

2. SITUS WEB, DATA DAN AKUN DIGITAL

a. Perhatikan juga keamanan akses kata sandi dan 2 *Factor Authentication* dalam setiap akun digital Anda!

Jangan lupa keluar (*sign out*) dari akun Anda ketika sudah selesai menggunakan. Terutama dalam gawai yang digunakan bersama seperti komputer kantor atau keluarga.

b. HTTP/HTTPs dan Keamanan Situs

HTTP/HTTPs adalah protokol komunikasi dalam situs yang perlu Anda cek sebelum mengakses.

Apa perbedaan antara HTTP dan HTTPs?

HTTP merupakan **protokol yang terbuka** dan memudahkan seseorang untuk mengetahui informasi yang Anda kirimkan, seperti *username* dan kata sandi.

HTTPs merupakan **protokol komunikasi yang tertutup**. Informasi mengenai *username* dan kata sandi akan dienkripsi sehingga pihak lain tidak dapat melihat.

Untuk dapat mengetahui apakah sebuah situs menggunakan protokol HTTP atau HTTPs Anda dapat meng-*install* "**HTTPs Everywhere**" di peramban milikmu.

c. **Pengelolaan Data di *Cloud Storage***

Dalam mengelola data di *cloud storage*, seperti Google Drive atau Dropbox, audit akses berkas data dan akun yang dibagikan pada orang lain – keluarga atau rekan kerja – dan pastikan semua akses ini aman.

Pertimbangkan memberikan kata sandi atau membatasi waktu pengaksesan saat pada saat pembagian akses.

Perhatikan juga aplikasi dan akun yang terkait dengan penyimpanan data Anda. Matikan akses aplikasi pihak ketiga yang tidak rutin Anda gunakan (Anda selalu bisa memberi akses kembali ketika Anda butuh.

Jangan lupa non-aktifkan akses dari gawai yang sudah tidak dipakai!

3. PERILAKU AMAN

Dalam situasi digital, melakukan tindak pencegahan atau mengurangi risiko dengan menjaga dan mengelola "tubuh digital" melalui berperilaku aman lebih baik!

Menjaga dan mengelola "tubuh digital" melalui berperilaku aman lebih baik!

Apa yang bisa dilakukan?

- **Pilih perangkat ataupun aplikasi yang mengedepankan privasi dari penggunanya.**
  Tips: Saat meng-*install* aplikasi, baca syarat dan ketentuan penggunaan serta bagaimana data kita dikumpulkan, dikelola, dan didistribusikan kepada pihak lain.

- **Pilih perangkat ataupun aplikasi yang menerapkan enkripsi.**
  Tips: Lakukan juga enkripsi untuk data-data yang sensitif, termasuk pada PII yang vital dan berkas kerja.

- **Gunakan perangkat ataupun aplikasi yang sistemnya paling terbaru.**
  Tips: Selalu perbaharui sistem operasi (OS) dari gawai ataupun aplikasi yang digunakan.

- **Cek jejak digital yang beredar secara reguler, utamanya PII/data pribadi yang vital dan sensitif.**
  1. Lakukan pengecekan sederhana dengan mencari nama lengkap atau panggilan khas melalui mesin pencarian Google. Lakukan ini dengan *browser* atau peramban dalam mode penyamaran (*incognito* atau *private*) sehingga hasil pencarian tidak dipersonalisasi sesuai dengan preferensi kita oleh Google.

2. Cek apakah ada informasi sensitif yang perlu dihapus? Apakah ada data pribadi yang dulu Anda nyaman untuk sebarkan, namun kini tidak nyaman lagi bila diakses orang yang tidak dikenal?

Tips: Batasi informasi pribadi yang dimuat di internet dan media sosial dengan menyelidiki jejak digital Anda yang dapat diperoleh di internet dengan mudah.

- **Deaktivasi akun-akun digital yang sudah tidak digunakan.**
  Tips: Pertimbangkan untuk langsung menghapus akun tersebut jika memang tidak akan pernah dipakai. Sebelum deaktivasi atau menghapus akun digital, jika diperlukan Anda bisa mengunduh data-data Anda selama menggunakan akun digital tersebut terlebih dulu. Opsi ini biasa disediakan oleh masing-masing *platform* digital.

- **Pisahkan akun digital atau media sosial pribadi dengan àkun pekerjaan dan/atau akun yang mengandung informasi sensitif.**
  Tips: Gunakan akun email yang dapat dibuang untuk kepentingan membuat akun yang bersifat sementara.

- **Segera hancurkan informasi pribadi yang diperlukan untuk kepentingan sementara ketika sudah tidak diperlukan lagi.**
  Tips: Saat melakukan pengumpulan data pribadi orang lain untuk tujuan tertentu, misalnya untuk berkas administrasi acara, segera hapus dengan aman begitu tujuan pengumpulan data tersebut selesai, sehingga tidak membawa risiko bagi orang lain.

- **Setel pengaturan keamanan dan privasi di setiap**
  Tips: Sesuaikan fitur-fitur keamanan dan privasi sesuai dengan level keamanan dan kenyamanan. Perhatikan juga bahwa di balik sebuah kenyamanan ada keamanan yang sedang kita kompromikan.

4. MENGHADAPI ANCAMAN YANG TERJADI

Prinsip utama ketika mengalami ancaman atau serangan adalah **memprioritaskan keamanan diri dan orang terdekat, serta melakukan pendokumentasian bukti dan kronologi serangan**. Langkah-langkah selanjutnya ditentukan sesuai dengan kebutuhan dan situasi yang dihadapi.

a. Kebocoran Data atau Akses Gawai

i. Penyadapan

Jalur komunikasi yang disusupi pihak lain tanpa sepengetahuan dan persetujuan dari pihak-pihak yang melakukan komunikasi.

Indikatornya beragam, seperti:

1. Informasi yang kebocoran tidak diketahui, bunyi statis yang terus-terusan terjadi saat panggilan suara dilakukan.
2. Baterai ponsel yang lebih cepat habis daripada biasanya padahal tidak digunakan.
3. Penggunaan paket data yang lebih dari biasanya padahal tidak ada perubahan penggunaan.
4. Ponsel yang melakukan aktivitas mencurigakan seperti: menginstal aplikasi lain secara otomatis atau nyala dan mati dengan sendirinya tanpa ada pengaturan otomatis, dan lainnya.

ii. **Pembobolan Fisik**

Ponsel atau laptop yang pernah diakses oleh orang lain yang tidak dipercaya, misalnya mengalami pencurian atau penyitaan gawai, dan lalu disusupi sesuatu (seperti aplikasi pengintai) atau diduplikasi datanya tanpa sepengetahuan dan persetujuan pemiliknya.

Hal-hal yang dapat dilakukan saat mengalami penyadapan atau pembobolan fisik:

- Matikan dan hentikan menggunakan perangkat tersebut untuk sementara waktu.
- Gunakan jalur komunikasi lain yang sudah terenkripsi atau memiliki fitur *end-2-end encryption*. Hindari penggunaan SMS atau panggilan telepon biasa (GSM).
- Lakukan reset data pabrik (*factory reset*) atau penghapusan data (*data wipe*) pada perangkat **sebanyak beberapa kali** sebelum menggunakan perangkat tersebut kembali. Lakukan opsi ini setelah melakukan *back-up* data-data penting.
- Hubungi layanan digital forensik independen yang ada untuk konsultasi bila diperlukan.

iii. Phishing

Pencurian data dan akses sensitif melalu penipuan atau memperdaya target sehingga seakan-akan telah menyerahkan data pribadinya atau bahkan uang pada pihak yang terpercaya.

Contoh: dikirimi formulir pendaftaran kegiatan palsu yang meminta *file copy* KTP, CV, atau dikirimi tautan palsu yang tampilan lamannya menyerupai situs resmi yang membutuhkan informasi *login* berupa *username* dan kata sandi.

Hal-hal yang dapat dilakukan saat mengalami phishing:

- Segera ganti seluruh kata sandi.
- Cek seluruh transaksi keuangan jika informasi yang dapat diakses pelaku termasuk akun-akun keuangan (misal: kata sandi *m-banking*).
- Hubungi *customer service* resmi untuk melakukan pemblokiran akun sementara jika diperlukan.
- Lakukan pemindaian sistem (*system scan*) pada perangkat yang digunakan.

iv. Peretasan

Ada pengaksesan akun atau data tanpa sepengetahuan dan persetujuan (tanpa otoritas) pemilik akun, *platform*, atau data.

Hal-hal yang dapat dilakukan saat mengalami peretasan:

- Segera ganti seluruh kata sandi.
- Laporkan kejadian pada *platform* digital terkait agar dapat mengambil alih akun, atau untuk menghapusnya.
- Lakukan pemindaian sistem (*system scan*) pada perangkat yang digunakan.

b. Pelacakan Lokasi dan *Surveillance*

Hal ini dapat dilakukan dengan berbagai cara, seperti dari dari aplikasi *spyware* yang di-*install* secara diam-diam, pengamatan fitur geolokasi ponsel/*geotag* aplikasi yang diaktifkan, memperhatikan CCTV atau bahkan memantau transaksi keuangan terakhir bila pelaku memiliki aksesnya.

Hal-hal yang dapat dilakukan saat mengalami pelacakan lokasi atau pengawasan:

- Matikan fungsi GPS.
- Lakukan pemindaian sistem (*system scan*) pada perangkat yang digunakan.
- Matikan dan hentikan menggunakan perangkat tersebut untuk sementara waktu.
- Lakukan penyamaran saat beraktivitas menggunakan akun digital, misal dengan mengaktifkan VPN, menggunakan akun anonim, menggunakan *burner phone* (ponsel sekali pakai), dll.
- Lakukan penyamaran fisik jika terkait aktivitas fisik yang dapat diawasi melalui CCTV.

c. Virus, *Malware*, *Spyware*

Ketiga hal ini bisa disusupi ke dalam perangkat digital dengan berbagai cara, misal disisipkan pada unduhan ataupun saat mengklik tautan yang tidak dapat dipercaya. Ketiganya dapat digunakan untuk mencuri data, pengintaian, ataupun perusakan data.

Hal-hal yang dapat dilakukan saat menghadapi virus, *malware*, *spyware*:

- *Install* dan selalu perbaharui anti-virus dan anti-*malware* pada perangkat yang digunakan.

REKOMENDASI Investasi pada keamanan digital dengan menggunakan anti-virus dan anti-*malware* berbayar yang memiliki fitur menjaga keamanan perangkat lebih lengkap.

d. Serangan DDoS (*Distributed Denial-of-Service*)

Jenis serangan ini dilakukan dengan cara membanjiri lalu lintas jaringan internet pada *server*, sistem, atau jaringan sampai tidak dapat diakses.

Hal-hal yang dapat dilakukan saat mengalami serangan DDOS:

- Berkoordinasi dengan tim IT, termasuk penyedia layanan *web* (*hosting* atau *domain*) terkait dengan hal-hal seperti: situasi yang dihadapi, kapan serangan terjadi, aset apa saja yang terdampak, dampak pada pengguna atau audiens, dan langkah-langkah selanjutnya.

e. *Doxxing*

Upaya pencarian dan pembocoran data pribadi seseorang ke ruang publik, misal di media sosial, untuk tujuan jahat. *Doxxing* biasa diikuti dengan tindak perundungan, intimidasi, bahkan sampai persekusi (penganiayaan).

f. Perundungan, Intimidasi, Persekusi

Dari serangan pada perangkat digital seperti peretasan, pemantauan, hingga serangan dalam bentuk ancaman atau pelecehan berulang yang dilakukan melalui jalur komunikasi publik (misal: akun media sosial publik) dan privat (misal: nomor ponsel), baik secara personal maupun ditujukan langsung pada keluarga atau orang terdekat).

Hal-hal yang dapat dilakukan saat mengalami *doxxing*, perundungan, intimidasi, persekusi:

- Dokumentasikan serangan dengan menyimpan screenshot dan URL/Tautan dari postingan atau akun yang melakukan *doxxing*, perundungan, intimidasi, ataupun persekusi daring.
- Buat kronologi serangan.
- Laporkan postingan dan akun yang menyebarkan data pribadi tersebut ke *platform* digital terkait agar dapat segera dihapuskan.
- Amankan seluruh akun digital yang dimiliki, seperti dengan ganti kata sandi, aktifkan 2FA bila belum. [LANJUT KE HALAMAN BERIKUTNYA]

- Tingkatkan pengaturan privasi, bila perlu kunci akun digital yang dimiliki atau buat jadi privat untuk mengurangi risiko perundungan atau intimidasi daring.
- Hindari berkomunikasi dengan akun-akun yang melakukan perundungan.
- Jika memilih untuk kunci atau privat akun digital, lakukan penyaringan *followers*/daftar pertemanan sehingga hanya oleh orang yang dikenal saja.
- Lakukan hal serupa untuk akun digital orang-orang terdekat kita.
- Pertimbangkan untuk mengakses rumah aman bila ada risiko serangan juga ditujukan secara langsung.

g. Perusakan Reputasi

Penyalahgunaan data pribadi atau jejak digital korban yang berhasil diakses pelaku baik yang terbaru maupun dari masa lalu, ataupun dengan melakukan manipulasi data/narasi.

h. Kriminalisasi

Upaya pemidanaan melalui jejak digital yang ada atau dimanipulasi.

Hal-hal yang dapat dilakukan saat mengalami perusakan reputasi atau kriminalisasi:

- Dokumentasikan perusakan reputasi yang dilakukan dengan menyimpan *screenshot* dan URL/Tautan dari postingan atau akun yang melakukannya.
- Laporkan postingan dan akun yang melakukan perusakan reputasi jika mengandung pelanggaran standar komunitas platform digital.
- Lakukan analisis pemetaan risiko bila ingin klarifikasi ataupun konfrontasi.

5. LAPOR!

Menerima serangan digital?

1. Lakukan pemetaan risiko dan prioritaskan keselamatan diri atau orang-orang terkait.

2. Lakukan mitigasi awal, misal keluar dari grup-grup percakapan sensitif jika terindikasi ada penyadapan, peretasan, dan lainnya.

3. Buat kronologi mencakup detail serangan, perangkat atau akun digital yang diserang, bentuk serangan, dan lainnya yang dirasa perlu.

4. Laporkan ke kanal-kanal di halaman setelah ini!

SAFEnet

- Mengisi formulir daring di https://s.id/laporserangan
- Mengirim email ke aduan@safenet.or.id
- Mengontak *hotline*, WhatsApp, atau Telegram di +62 8119223375
- Mengabari langsung lewat *direct message* ke IG atau Twitter @SAFEnetVoice

PurpleCode Collective

- Mengirim email ke help@purplecodecollective.net

Keamanan Organisasi/ Sistem

Ketika aktivitas pembela HAM dilakukan dalam lingkup organisasi, isu keamanan digital menjadi lebih kompleks. Gerakan masyarakat sipil perlu secara sadar dan berpikir dengan luas mengenai keamanan dan risiko organisasi. Keamanan yang holistik harus melibatkan setiap anggota dan tim kerja organisasi dan menjadi bagian integral dalam alur kerja secara berkelanjutan.

Keamanan yang holistik harus melibatkan setiap anggota dan tim kerja organisasi.

Salah satu upayanya dengan menciptakan **Standar Operasional Prosedur** terkait **Keamanan dan Resiko Lembaga**. SOP Keamanan dan Resiko ini tidak baku, tiap lembaga memiliki kerentanan dan kebutuhan yang berbeda-beda. Dalam buku saku ini akan dijelaskan beberapa hal penting dalam menyusun SOP Keamanan.

Lakukan Analisis Risiko Organisasi

Coba anda identifikasi apa saja aset kunci organisasi dalam segala aktivitas digital. Hal ini akan berdampak besar pada strategi keamanan yang perlu diterapkan dalam organisasi. Coba buat ulang daftar ini pada catatan Anda sendiri.

INVENTARISASI ASET INFORMASI

Salah satu bagian utama yang berada dalam risiko serangan digital adalah informasi, yang perlu diinventarisasi oleh organisasi Anda. Coba klasifikasikan apa saja bentuknya!

Aset Informasi	
Dokumen elektronik	
Sistem informasi atau *database*	
Data pribadi anggota (PII)	
Dokumen fisik	
Media penympanan (*flashdisk*, *harddisk*, dll)	
Informasi verbal	
Surat elektronik	

IDENTIFIKASI ASET DAN APLIKASI

Berhubung panduan ini secara khusus membahas aktivitas digital, coba inventarisasikan apa saja media dan kanal tempat aset-aset informasi tersebut disebarkan atau disimpan!

1	**Handphone, Laptop, PC (*Personal Computer*), penyimpanan data (*flashdisk*, dll) dan gawai lain**	
	Gawai eksklusif kantor	
	Gawai personal anggota	
2	**Media sosial**	
	Facebook	
	Instagram	
	Twitter	
	Dll., sebutkan	
3	**Layanan surel**	
	Gmail	
	Yahoo mail	
	Hotmail	
	Dll., sebutkan	
4	***E-banking***	

5	***File sharing* atau *cloud storage***	
	Google Drive	
	Dropbox	
	Dll., sebutkan	
6	**Aplikasi pesan**	
	LINE	
	Telegram	
	WhatsApp	
	Dll., sebutkan	
7	**Aplikasi lain**	
	Aplikasi perencanaan kerja (Asana, Slack, dll)	
	Aplikasi transportasi (Gojek, Grab, dll)	
	Aplikasi konferensi video (Google Classroom, Zoom, Jitsi, dll)	
	Dll., sebutkan	

KLASIFIKASI INFORMASI KUNCI YANG DIMILIKI ORGANISASI

Setelah menginventarisasi aset, coba klasifikasikan aset informasi organisasimu.

Biasanya, ada dua jenis klasifikasi informasi yakni: a) **Kritikal** sebagai informasi kritikal yakni data organisasi yang dibutuhkan untuk operasional kerja. Seperti kontrak, data keuangan atau asuransi; b) **Informasi Sensitif** adalah data yang jika diakses oleh pihak yang tidak berwenang atau tidak berkepentingan dapat membahayakan organisasi, pekerja, dan jaringan organisasi.

Berdasarkan dua parameter tersebut, kategorikan aset informasi organisasi pada beberapa tingkatan, misalnya:

RAHASIA

Tingkat kerahasiaan maksimal

TERBATAS

Tingkat kerahasiaan menengah

INTERNAL

Tingkat kerahasiaan rendah

PUBLIK

Terbuka untuk umum

IDENTIFIKASI ANCAMAN

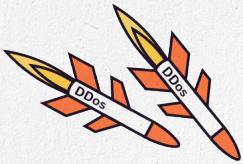
Jika Anda sudah melakukan *checklist* aset, saatnya bagi Anda untuk mengetahui apa saja ancaman kebocoran dan serangan yang dihadapi aset organisasi. Berikut daftar ancamannya:

1. Penyadapan atau pembobolan fisik

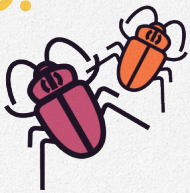
2. *Phishing*

3. Peretasan

4. Peretasan web atau disrupsi *traffic* web (DDoS)



5. Virus, *Malware*, *Spyware*



6. Pelacakan lokasi dan *surveillance*

7. Intersepsi komunikasi

Selain itu, pertimbangkan juga risiko digital yang berkaitan tapi tidak secara penuh termasuk dalam keamanan informasi, seperti:

1. Perisakan (*bullying*), intimidasi, dan serangan terhadap kesehatan mental anggota organisasi.
2. Kriminalisasi atau pemblokiran konten digital.

Setelah Anda mengidentifikasi aset dan ancaman, waktunya Anda mempertimbangkan penyusunan strategi keamanan organisasi!

Manajemen Manusia

1. Upayakan ada proses *screening* terhadap latar belakang pekerja. Khususnya pekerja yang memiliki akses terhadap informasi rahasia.

2. Persiapkan sistem pengawasan dan penegakan aturan agar setiap individu mempraktikkan sistem keamanan dengan baik. Bergantung pada faktor risiko, ini bisa melingkupi aktivitas digital personal mereka di luar lingkungan pekerjaan.

3. Ketika diperlukan, buat perjanjian kerahasiaan (*non-disclosure statement*) yang mengikat secara hukum ketika pekerja mendapatkan akses terhadap informasi rahasia yang bersifat vital.

4. Pastikan bahwa setiap perubahan status pekerja (diangkat sebagai pekerja, berganti posisi, keluar/dipecat, dll) diketahui oleh administrasi. Pastikan bahwa kebijakan akses pekerja semua pekerja langsung disesuaikan.

5. Pastikan organisasi memiliki sistem perlindungan dan dukungan terhadap pekerja jika mereka menjadi target dari serangan digital. Termasuk dalam segi kesehatan mental.

6. Lakukan pelatihan dan pendidikan terkait keamanan digital kepada anggota organisasi. Strategi keamanan ini harus bersifat holistik; praktik buruk satu orang bisa menggagalkan strategi keamanan secara keseluruhan.

Kebijakan Akses

Kebijakan ini bertujuan untuk mengawasi jalur terhadap aset organisasional untuk melindungi keamanan individu pembela HAM dan jaringannya, termasuk hal-hal yang sedang dikerjakan.

1. AKSES KE TEMPAT KERJA

Kebijakan mengenai akses ke tempat kerja ini perlu diperhatikan dalam menjaga keamanan digital, karena segala informasi terkait aktivitas pekerjaan kita terdapat pada area ini.

a. Kantor dan Meja Kerja

i. Perhatikan siapa saja yang memiliki akses ke kunci atau PIN kantor

- Catat siapa saja yang memiliki kunci duplikat atau akses PIN kantor.
- Kumpulkan kunci dari staf yang sudah tidak bekerja di kantor tersebut dan ganti ganti PIN atau hapus akses PIN orang tersebut.
- Jangan meminjamkan kunci kantor kepada seseorang yang bukan staf tetap termasuk membagikan PIN kepada staff tidak tetap.

ii. Mengunci meja, pintu, & lemari

- Pastikan ada orang yang bertanggung jawab mengunci kantor (penjaga kantor atau orang terakhir yang pulang dari kantor).
- Simpan dokumen dalam lemari atau laci yang dapat dikunci.

iii. Pengaturan meja kerja

- Posisikan meja kerja agar tidak membelakangi pintu dan membelakangi lalu lintas orang agar layar komputer tidak mudah diintip.

b. Akses Keluar dengan Pintu Darurat

- Kantor yang ideal memiliki akses keluar darurat, tidak hanya memiliki satu akses keluar.
- Selalu cek kondisi kunci dari pintu darurat.

c. Kerja dari Rumah atau Ruang Kerja Personal

- Buat kesepakatan terkait keamanan dengan orang yang tinggal di rumah.
- Batasi akses orang asing terhadap ruang kerja, jika sangat dibutuhkan, pastikan amankan gawai dan semua dokumen.

2. AKSES KE DOKUMEN FISIK

a. Dokumen Cetak

- Tidak disarankan untuk membawa pulang dokumen rahasia versi cetak.
- Hindari untuk meninggalkan dokumen cetak di atas meja tanpa pengawasan.
- Simpan dokumen cetak di lemari yang terkunci sebelum pulang.

b. Penghancuran Dokumen

- Hancurkan dokumen yang sudah tidak diperlukan lagi dengan mesin penghancur kertas sesegera mungkin.
- Hancurkan informasi pribadi yang terdapat pada paket yang dikirim ke alamat kantor/rumah.

3. PERANGKAT

Perangkat di sini adalah ponsel, laptop, atau komputer, termasuk kamera yang digunakan untuk bekerja atau menyimpan dokumen berkaitan dengan pekerjaan.

a. Jumlah Perangkat

- Kurangi jumlah perangkat yang terkoneksi dengan informasi pekerjaanmu, seperti alamat email kerja.

- Tidak disarankan untuk membawa pulang dokumen rahasia versi cetak.
- Setiap perangkat baru dengan akun kerja atau menyimpan data yang berkaitan dengan pekerjaan membutuhkan perlindungan dari kehilangan, pencurian atau peretasan. Jika memungkinkan, ponsel dan komputer (laptop atau komputer personal) merupakan kedua perangkat yang digunakan untuk pekerjaan.
- Jika memungkinkan, organisasi menyediakan laptop atau komputer bagi staf untuk memastikan informasi pekerjaannya hanya ada di perangkat tersebut dan dipisahkan dari perangkat pribadi pekerja.
- Gunakan ponsel yang berbeda dari ponsel pribadi untuk urusan media sosial organisasi, untuk meminimalisir risiko serangan digital terjadi secara terpusat pada 1 perangkat.

b. Akses ke Perangkat

- Pastikan Anda adalah satu-satunya orang yang dapat mengakses dokumen kerja. Jika ada data rahasia pada perangkat yang sama dengan pihak di luar organisasi, usahakan untuk hapus.

- Pasang kata sandi, PIN atau sandi berbentuk frasa/kalimat untuk mengakses setiap perangkat yang menyangkut informasi organisasi termasuk ponselmu.
- Ketika enkripsi perangkat tersedia, biasakan untuk mengunci layar. [Lihat lebih rinci terkait enkripsi dokumen]

4. AKSES KE INTERNET

Pastikan Anda menggunakan akses internet yang terpercaya ketika mengakses dokumen pekerjaan.

Akses internet terpercaya adalah jaringan yang dengan mudah dapat Anda ketahui pengelolanya dan hanya mereka yang dapat mengaksesnya.

Hati-hati di internet.

Cobalah untuk lebih perhatikan beberapa surel yang Anda curigai sebagai phising. Jika Anda menerimanya atau mungkin menduga sebuah surel sebagai *phishing* karena tidak otentik, maka **jangan buka tautan/pranala atau**

mengunduh apapun dari lampiran tersebut. Segera hubungi atau laporkan ke sekretariat organisasi. Setelah melaporkan ke pihak organisasional, sebarkan salinan email dengan **notifikasi** sebagai surel yang mencurigakan dan peringatkan rekan kerja untuk tidak membuka jika menerima surel serupa. Sederhananya, jangan buka dan unduh tautan dan beritahu rekan kerja untuk saling jaga!

KONEKSI INTERNET TERPERCAYA

Rumah

Kantor

Coworking Space yang diketahui pengelolanya

KONEKSI INTERNET TIDAK TERPERCAYA

Bandara

Kafe

Perpustakaan

Layanan wifi gratis di berbagai daerah dan tempat umum (seperti: JAKWIFI/WIFI ID, wifi pusat perbelanjan)

5. AKSES KE AKUN DIGITAL

a. Otentikasi 2 Langkah (2FA)

Pastikan setiap anggota mengikuti prinsip otentikasi 2 langkah dalam mengakses akun-akun kantor! Cek kembali soal ini di bagian ini.

b. Manajemen Kata Sandi

Pastikan kata sandi yang dibuat bersifat aman, baik kata sandi anggota organisasi maupun akun organisasi. Baca kembali panduannya di sini.

i. Sandi tim

- Organisasi dapat mempertimbangkan untuk menyimpan kata sandi organisasi di aplikasi Password Manager, sehingga menghindari menyimpan kredensial secara tidak aman (melalui surel, mencatat di catatan, dan lainnya).
- Kata sandi organisasi atau tim yang dimaksud adalah kata sandi untuk akun yang digunakan oleh lebih dari 1 orang, misalnya akun media sosial untuk kampanye, atau akun email untuk *hotline*.

ii. *Password manager*

- Untuk mengelola akun dan kata sandi Anda dan memastikan bahwa semua kata sandi aman (panjang, kuat, unik), gunakan aplikasi *password manager*!

- Salah satu pilihan baik adalah KeePassXC. Untuk Windows, macOS, Linux, ia dapat diunduh di sini.
- Panduan penggunaan KeePassXC sebagai password manager dapat dilihat di sini.
- Untuk pengguna Android dan iOS dapat menggunakan aplikasi lain:
  Android: KeePass2Android, KeePassDX
  iOS: KeePassium, Strongbox
- Perlu menjadi catatan bahwa aplikasi yang disarankan ini berdasarkan prinsip teknologi yang terbuka dan gratis (*free and open source*) dan akan terus diperbaharui. Untuk informasi terkait *free and open source software* lihat ini.

iii. Berbagi kata sandi

- Jika Anda harus membagikan kata sandi dengan kolega, gunakan strategi berbagi yang aman untuk mengurangi risiko pencurian. Praktik ini hanya digunakan untuk akun yang memang digunakan secara bersama, bukan akun pribadi.
- Sandi dapat diberikan melalui kertas untuk langsung dimasukkan ke Password Manager penerima. Jangan lupa menghancurkan kertas tersebut.

- Menggunakan layanan pihak ketiga seperti **Key Vault** tidak disarankan karena Anda membagikan kata sandi dengan pihak ketiga dan jaringan mereka. Konten (sandi) tidak menggunakan teknologi *end-to-end encryption*, yang memastikan konten hanya dapat diketahui oleh pihak pengirim dan penerima.
- Penggunaan aplikasi pesan yang menggunakan teknologi *end-to-end encryption* seperti Signal dan Wire dapat menjadi opsi.
- Ketahui lebih lanjut mengenai komunikasi *end-to-end encryption* pada bagian Praktik dan Kebijakan Komunikasi.

c. Perubahan Akses ke Aset Organisasi

- Jangan lupa buat kebijakan penghapusan akses bagi seorang staf yang akan berhenti.
- Bagian `operasional/sekretariat perlu memastikan staf tersebut memasang notifikasi di akun emailnya bahwa yang bersangkutan sudah tidak lagi bekerja di organisasi Anda.
- Pastikan staf yang sudah tidak lagi bekerja tersebut menyediakan kontak kolega yang dapat dihubungi.
- Email akan tetap aktif selama (waktu tertentu), setelah itu akan dimatikan.

- Semua properti organisasi yang digunakan harus dikembalikan, termasuk kunci kantor jika ada.

6. KEBIJAKAN MANAJEMEN DATA (RS)

a. *Back-up* Data

- *Back-up*/cadangan dokumen dan sistem dapat disimpan dalam media eksternal, seperti *hard disk* eksternal dan USB. Pastikan Anda telah mengenkripsi dokumen yang ingin di-*back-up* pada media eksternal.
- Lakukan *back-up* secara rutin, minimal 1 bulan sekali. *Back-up* juga dapat dilakukan sebelum Anda melakukan perjalanan dinas atau meeting ke tempat yang berisiko tinggi.
- Informasi mengenai enkripsi *file* dapat dilihat di bawah ini:
  Aplikasi untuk mengenkripsi file: Veracrypt
- Informasi terkait strategi melakukan *back-up* untuk macOS dan iOS.
  macOS seri X: Time Machine
  iOS
- Enkripsi *hard disk*/USB untuk tempat *back-up*.
  Cara backup: MacOS, iOS, Windows, Android, Linux

b. Transfer Data

- Mentransfer informasi rahasia dapat dilakukan hard disk eksternal yang diberikan secara segera dengan terlebih dahulu mengenkripsi dokumen. Pengiriman dapat juga dilakukan melalui email yang terenkripsi.
- Pastikan untuk memberitahu semua pihak yang dituju akan adanya dokumen yang dikirim sebelum mereka mengaksesnya. Mengetahui bahwa akan ada file yang diterima dapat membantu mencegah upaya phishing yang menggunakan lampiran sebagai sumber *malware*.

c. Surel

- Gunakan surel yang terenkripsi untuk melakukan transfer data.
- Jika menggunakan surel yang tidak terenkripsi, jangan lupa enkripsi *file* yang ingin dikirim terlebih dahulu.
- Beri notifikasi kepada pihak penerima bahwa Anda akan mengirim surel dan menyertakan *file*.
- Pahami bahwa informasi mengenai subjek, kepada, dan dari tidak terenkripsi, sehingga jangan pernah menampilkan informasi yang bersifat pribadi di sana.
- Jika ingin mengirim *file* dalam jumlah besar, hindari penggunaan WeTransfer karena *file* yang akan dikirim tidak tersimpan secara terenkripsi.

- Disarankan untuk menggunakan Tresorit Send, karena layanan tersebut memiliki fitur *end-to-end encryption* dalam pengiriman *file*-nya. Tresorit Send dapat digunakan untuk mengirim *file* hingga sebesar 5GB.

d. Media Eksternal

- Cek pemilik dan pengguna terakhir USB/*hard disk* eksternal sebelum digunakan.
- Pastikan komputer/laptop anda memiliki anti-virus sebelum memasukkan media eksternal.
- Hindari mencolokan media eksternal apapun ke komputer/laptop Anda tanpa mengetahui asal dan pemiliknya.
- Media eksternal apapun dapat digunakan untuk mentransfer data, tetapi setelah transfer, data tersebut harus dihapus dari media eksternal. Enkripsi dahulu *file* rahasia atau seluruh *drive*.

e. Menghapus Data

- Informasi yang dihapus masih memiliki kerentanan untuk dapat dipulihkan jika tidak "ditimpa" secara khusus.
- Setelah menghapus dokumen, pastikan hapus juga secara permanen dari *recycle bin* atau *trash*.

- Jika *file* tersebut sangat penting dihapus permanen maka pastikan untuk menggunakan praktik penghapusan yang aman. Tips menghapus *file* yang aman dapat dilihat di tautan berikut:
  MacOS: *How to Delete Your Data Securely on macOS*
  Windows: *How to Delete Your Data Securely on Windows*

f. Enkripsi Perangkat

i. Enkripsi gawai

- Jika gawai Anda hilang atau dicuri, enkripsi perangkat (disebut juga sebagai *Full Disk Encryption*) akan melindungi komputer, ponsel, dan gawai lain dari akses data secara fisik dengan cara mengenkripsi *hard drive*.

- Fungsi enkripsi hanya akan berjalan ketika perangkat dalam keadaan mati. Enkripsi tidak berfungsi jika Anda hanya menon-aktifkan sementara (*sleep mode*) komputer atau laptop Anda. Lakukan enkripsi perangkat (*Full Disk Encryption*) di semua perangkat yang berisi informasi organisasi dan akses terhadap akun organisasi (seperti surel).

- Informasi terkait cara melakukan enkripsi untuk ponsel dan tablet dapat dilihat pada tautan berikut ini:
  Android: Artikel 1, Artikel 2
  iOS: Apple Support, Artikel

- Informasi terkait cara mengenkripsi laptop atau komputer dapat dilihat pada tautan berikut:
  Windows dengan BitLocker
  Mac dengan FileVault
  Linux: diaktifkan ketika menginstall Sistem Operasi

ii. Enkripsi media eksternal

- Jika USB, *hard drive*, atau media eksternal lainnya berisi media sensitif atau informasi rahasia, pastikan benda tersebut dienkripsi dan disimpan di tempat yang aman.

- Informasi mengenai cara mengenkripsi dokumen dengan sistem operasi yang Anda gunakan dapat dilihat pada tautan berikut:
  Mac: enkripsi dengan FileVault
  Windows: enkripsi dengan Veracrypt
  Linux: enkripsi dengan Veracrypt

7. PERJALANAN DINAS KE LUAR DAERAH/NEGERI

Perjalanan dinas memungkinkan Anda lebih 'terungkap' ke publik, baik secara individu, perangkatmu, dan dokumen-dokumen pekerjaanmu. Termasuk potensi kehilangan, pencurian, penyitaan, atau pengrusakan laptop atau perangkat lainnya.

Jika sedang melakukan perjalanan dinas, pastikan beberapa hal penting di sekitar negara atau daerah yang Anda tuju. Termasuk peraturan daerah atau kebijakan lokal lainnya. Langkah keamanan terkait perjalanan dinas harus diambil baik di tingkat organisasi dan individu khususnya berkaitan dengan komunikasi dan perangkat kerjamu.

a. Untuk Organisasi

- Jika memungkinkan sediakan sumber daya atau dana untuk asuransi perjalanan dinas bagi pekerja.
- Lakukan analisis resiko dan potensi *surveillance* terhadap wilayah kerja (kota atau negara), mulai dari kebijakan tentang visa atau pengecekan di imigrasi di tiap-tiap negara.

- Prosedur dan formulir keamanan khusus mengenai perjalanan dinas yang mencakup: komunikasi rutin dengan waktu yang ditentukan (*check-in* staf), menyediakan perangkat (laptop dan ponsel) khusus yang bisa dibawa bepergian untuk bekerja, memastikan adanya organisasi atau mitra lokal untuk membantu.

b. Untuk individu yang Bepergian

Setiap perjalanan dinas sangat penting mengambil langkah pencegahan yang ekstra. Terutama mengenai informasi yang dapat dibawa atau disampaikan di sana. Hal ini berkaitan langsung dengan keamanan fisik, komunikasi, manajemen data dan perangkat yang akan dibawa dalam perjalanan.

Komunikasi dan Penggunaan Internet	Perangkat
• Penggunaan wifi publik yang tidak aman kerap kali tidak bisa dihindari, jika terpaksa menggunakan pastikan Anda selalu menggunakan VPN baik di perangkat ponsel, laptop, maupun tablet. • Hapus tembolok (*cache*), *cookie*, dan riwayat pencarian dan peramban. • Hapus kata sandi yang biasa Anda simpan otomatis di peramban baik di Chrome, Firefox, Safari. • Jika Anda melakukan transfer atau pengiriman data melalui surel. Pastikan Anda melakukan enkripsi pada pesan dan informasi yang penting.	• Sadari bahwa perangkatmu mungkin akan dicari, jadi pastikan Anda menerapkan prinsip keamanan perangkat sederhana: a) **enkripsi secara utuh** termasuk ponselmu, dan matikan perangkat ketika melintasi perbatasan; b) **buat cadangan file** di hard disk eksternal (yang juga terenkripsi), cek kembali kata sandi dan perangkatmu. • Ingat kembali manajemen data: bawa data seminimal mungkin. Usahakan untuk tidak membawa perangkat dengan data pribadi dalam perjalanan.

Sebuah tips untuk perjalanan dinas!

1. Pekerja HAM sering menghiasi laptopnya dengan stiker-stiker kampanye. Ternyata, kebiasaan tersebut berpotensi aparat atau petugas bandara misalnya dengan mudah mengidentifikasi identitasmu. Pertimbangkan untuk menyediakan sarung khusus ketika sedang berpergian!

2. Mengunggah status di media sosial memang sebuah kebebasan berekspresi, tapi pertimbangkan keamanan diri dan pekerjaanmu. Jangan lupa meminta persetujuan sebelum mengunggah foto mitra lokal atau orang-orang di sekitarmu. Jika ingin menyertakan lokasi, usahakan Anda unggah setelah Anda benar-benar pergi dari lokasi tersebut untuk menghindari penguntitan!

8. PRAKTIK DAN KEBIJAKAN KOMUNIKASI

Ketika berkomunikasi dengan rekan kerja, anggota organisasi, dan mitra, ketahuilah konteks yang sedang mereka hadapi. Cari tahu apakah mereka sedang melakukan perjalanan, di negara mana mereka sedang berada? Apakah akan membahayakan mereka jika menerima pesan melalui surel? Pastikan untuk memperhatikan bagaimana cara paling aman untuk berkomunikasi dengan mereka.

a. Komunikasi Daring

i. Surel

- Alamat tujuan (*To*) dan Dari (*From*) serta Subjek dalam surel, dapat terlihat oleh pihak ketiga selain penyedia layanan surel dan penerima yang Anda tuju, jadi hindari memasukkan informasi sensitif di bagian tersebut.

- Harap diperhatikan bahwa alamat surel kantor yang Anda gunakan dapat memberikan notifikasi kepada pelaku kejahatan mengenai keberadaan dari mitra atau penerima surel tersebut. Pertimbangkan saluran kontak lain jika menginginkan komunikasi yang tidak mencolok.

ii. Obrolan suara dan video

- Komunikasi suara dapat menjadi bentuk komunikasi yang cepat dan efisien, baik digunakan secara internal maupun dengan pihak eksternal. Untuk obrolan suara dan video dapat menggunakan Jitsi Meet karena menggunakan teknologi *end-to-end encryption*. Pilihan lainnya adalah menggunakan Wire, untuk konferensi video dapat memuat hingga 12 peserta dan untuk panggilan suara dapat memuat hingga 25 peserta.

- Hindari penggunaan Skype sebagai alat komunikasi video dan suara yang utama. Skype memiliki sejumlah praktik buruk yang mempermudah pengguna menjadi target atau disusupi, termasuk:
  Peniruan kontak yang mudah.
  Menjadi program yang terpisah dan bukan platform yang berjalan di peramban.

ii. Obrolan teks

- Untuk obrolan teks, prinsipnya sama dengan komunikasi suara dan video, pilih *platform* yang menggunakan teknologi *end-to-end encryption* dan terbuka.

- Prinsip teknologi *free and open source* penting agar teknologi yang digunakan dapat diaudit oleh publik.

- Untuk saat ini yang disarankan adalah Signal dan Wire. Keduanya juga memiliki aplikasi untuk digunakan di komputer atau laptop sehingga memudahkan untuk digunakan.
- Untuk mengetahui lebih lanjut mengenai dua aplikasi tersebut silakan cek tautan berikut.
  Cara menggunakan Signal untuk iOS di sini.
  Cara menggunakan Signal untuk Android di sini.
  Bagaimana Wire bekerja di sini.
- Unduh aplikasi tersebut dari sumber yang aman dan terpercaya.
  Tautan untuk unduh Signal di sini.
  Tautan untuk unduh Wire di sini.

b. Komunikasi dengan Kelompok Berisiko Tinggi

Penting untuk mengetahui konteks dan kondisi keamanan dari mitra yang akan Anda hubungi. Dalam upaya untuk melindungi mereka, upayakan untuk selalu mengikuti petunjuk mereka dalam berkontak, dan menyediakan pilihan saluran komunikasi.

c. Etiket *Web*

Saat mengunggah di media sosial secara publik, baik foto pribadi atau materi promosi kegiatan organisasi, perhatikan informasi pribadi lain yang mungkin terungkap.

- Cek izin dari pihak atau orang yang ada di gambar.
- Cek latar belakang foto apakah ada informasi pribadi seperti lokasi, kata sandi yang tercatat dalam *post-it* atau informasi pribadi lainnya seperti nama lengkap, nomor telepon, alamat surel, dll.

d. Tautan dan Lampiran

- Ketika hendak mengirim tautan dan lampiran, terlebih dahulu beri tahu penerima tentang pengiriman surel tersebut melalui saluran kedua seperti aplikasi pesan atau telepon.
- Pemberitahuan ini untuk memberikan jaminan kepada pihak penerima bahwa tautan dan lampiran tersebut bukan serangan *phishing*.
- Saat menerima tautan dan lampiran, pastikan cek kembali nama pengirim, konfirmasi melalui saluran terpisah kepada pengirim apakah mereka memang mengirim hal tersebut.

GLOSARIUM

***2-Factor-Authentification* (Autentikasi 2-Faktor)** Proses keamanan yang mengharuskan pengguna menggunakan setidaknya dua cara otentikasi yang berbeda. Misalnya kata sandi, sidik jari, dan kunci fisik. Istilah ini juga dikenal dengan nama lain 2-Step Verification (Verifikasi 2 Langkah).

***Back-up* (pencadangan)** Kopi dari data yang disimpan di suatu tempat, untuk mencegah kehilangan total jika terjadi kerusakan.

***Cloud storage* (komputasi awan)** Model penyimpanan yang meletakkan data digital dalam dalam *server*, dengan penyimpanan fisik yang diolah oleh perusahaan *hosting*. Perusahaan ini bertanggung jawab menjaga dan memastikan data dapat diakses dan diolah. Contohnya Google Drive.

DDoS (*Distributed Denial-of-Service*) Percobaan menghambat akses pengguna ke layanan daring, umumnya, dengan cara membanjiri jaringan dan memenuhi kapasitas proses *server* atau *bandwith*.

Doxxing Membeberkan identitas pribadi di muka publik, yang dapat berujung perundungan dan serangan, dan risiko keamanan secara umum.

End-to-end encryption Sistem komunikasi yang hanya mengizinkan dua pihak yang berkomunikasi untuk membaca pesan. Ia menghindarkan kebocoran informasi dari pihak ketiga, seperti penyedia jasa internet.

Enkripsi Proses pengkodean informasi, sehingga informasi tersebut hanya bisa diakses oleh pihak tertentu.

HTTP dan HTTPs "*Hypertext transfer protocol*", protokol standar yang mengizinkan peramban dan *server* untuk berkomunikasi dengan pertukaran data. Sementara HTTPs adalah protokol dengan ekstensi yang membuat koneksi terenkripsi antara *server* dan peramban.

***Malware* (*malicious software*)** Program atau perangkat lunak secara khusus didesain untuk menimbulkan kerusakan pada komputer, *server*, atau jaringan komputer.

Peramban (*browser*) Perangkat lunak yang digunakan untuk mengakses informasi dari internet. Ia mengambil informasi yang diperlukan dari *server* dan menampilkannya dalam gawai pengguna.

Peretasan (*hacking*) Dalam konteks digital, indakan yang memanfaatkan pengetahuan teknis untuk mengeksploitasi dan menembus sistem keamanan dan akses data tertentu.

Phishing Percobaan penipuan untuk memperoleh informasi sensitif dengan menggunakan identitas palsu, umumnya identitas terpercaya.

PII (*personal identifiable information*) Segala bentuk data yang dapat dimanfaatkan untuk mengidentifikasi orang tertentu, seperti nama panjang, nomor identitas, dan lainnya.

Spyware Perangkat lunak yang digunakan untuk mengeruk informasi orang atau organisasi dan mengirimnya pada pihak ketiga, dan mengancam privasi dan keamanan pengguna tersebut.

Surveillance Pemantauan dan pelacakan aktivitas, lokasi, atau perilaku.

Virus (komputer) Sejenis program komputer yang, ketika berjalan, menginfeksi komputer dengan cara mereplikasi diri dan menyisipkan kodenya ke program-program lain.

VPN (*virtual private network*) Jaringan privat yang dihadirkan untuk menyediakan anonimitas, privasi, dan keamanan dalam mengakses jaringan internet. Biasanya dikombinasikan dengan *proxy server* yang berfungsi sebagai jembatan dalam memenuhi permintaan data dari *server*.

panduan perlindungan digital untuk aktivis